WEST Search History

DATE: Thursday, December 04, 2003

Set Name side by side	Query	Hit Count	Set Name result set
DB=JPAB,EPAB,DWPI; THES=ASSIGNEE; PLUR=YES; OP=OR			
L7	L6 and (digital adj (licens$ or certificate))	2	L7
L6	((((obtain$ or deriv$ or get$ or find$) with key$)) with (certificat$ or license or signature)) and @pd<=19990327	128	L6
DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR			
L5	((((obtain$ or deriv$ or get$ or find$) with key$)) with (certificat$ or license or signature)) and @ad<=19990327	879	L5
L4	((((obtain$ or deriv$ or get$ or find$) with key$)) same (certificat$ or license or signature)) and @ad<=19990327	1142	L4
L3	L1 and (((obtain$ or deriv$ or get$ or find$) with key$)) same (certificat$ or license or signature)	1	L3
L2	L1 and (key$ same (certificat$ or license or signature))	2	L2
L1	6226618.pn. or 6151676.pn.	2	L1

END OF SEARCH HISTORY

WEST

End of Result Set

Generate Collection Print

L3: Entry 1 of 1 File: USPT Nov 21, 2000

DOCUMENT-IDENTIFIER: US 6151676 A
TITLE: Administration and utilization of secret fresh random numbers in a networked environment

US Patent No. (1):
6151676

Brief Summary Text (9):
A digital signature employing the El-Gamal algorithm utilizes the private key of the signer, a secret fresh random number, and generally the result of applying a secure hash function (such as SHA-1 or RIPEMD) to one or more data items, such as documents, files, programs, or keys (which for simplicity are referred to hereinafter as "documents") to manifest the signer's origination, approval, or certification thereof. The documents to which the signature applies are typically sent along with the signature unless they are already extant at or available to the recipient. At the receiving end a verification takes place which includes utilization of the originator's public key, which has been obtained by the recipient with a certificate from a trustworthy source, and application of the hash function to the documents which are received or otherwise available.

Brief Summary Text (10):
An encryption of data employing the El-Gamal algorithm for the purpose of transmission to a recipient generally involves using the public key of the recipient, which has been obtained with a certificate from a trustworthy source, and a secret fresh random number. The data so encrypted may comprise a symmetric key for one time use which has been used to encrypt in a computationally efficient manner an associated item employing a symmetric encryption algorithm, the encrypted symmetric key and the associated item constituting a package. At the receiving end, the encrypted data or package is decrypted by operations including a decryption using the private key of the recipient. In the case of a package, the decryption using the private key yields the symmetric key which is then used to decrypt the associated item in a computationally efficient manner.

Brief Summary Text (12):
In the aforementioned related patent application, it has been proposed that the private keys of users be maintained at the server in encrypted form, encrypted using user identifying keys, and supplied to the user or client equipment via the network only when needed, for example, for performing a digital signature or encryption. The user identifying keys are derived from user identifying information which is assumed to require the actual presence of the user at the user equipment, in particular a hash of a passphrase entered by the user or biometric information (fingerprint, voiceprint, retina scan, or face scan) measured or scanned by interaction with a physically present user.

Brief Summary Text (20):
From the point of view of the server, the present invention is directed to a method of administration of secret fresh random numbers for use by users in a networked environment to which a server is coupled, said method both assuring that the random numbers are secret and fresh and also being in the nature of a challenge response protocol in which: a user's ID is received via the network; at least a first random number is generated and encrypted using the public key of the user; a freshness

generating at least a first random number;

forming an encrypted component using the public key of the user, said encrypted component containing at least the first random number in encrypted form;

forming a freshness value corresponding to a current date/time;

hashing together items including the first random number and the freshness value to form a first hash;

forming a first signature of the first hash using the private key of the server;

sending to the user via the network a package including at least the encrypted component, freshness value, and first signature;

receiving a second signature of a second hash which has been formed by signing data from said package, derived at least from the first random number, said second signature being formed using the private key of the user; and

first verifying, using the public key of the user, whether the second signature is for the same first random number as was sent by the server.

9. A method for obtaining and using secret fresh random numbers at user equipment in a networked environment to which a server is coupled, there being associated with each user a unique respective set including an ID, a private key, and a public key corresponding to the private key, and with the server a private key and a public key, said method comprising, at the user equipment:

transmitting an ID of a user;

receiving a package including an encrypted component containing at least a first random number in encrypted form, which encrypted component has been produced using the private key of the user, a freshness value corresponding to a date/time, and a first signature of a first hash, said first hash having been formed by hashing together items including said first random number and the freshness value, and said first signature having been formed using the private key of the server;

decrypting the at least first random number using the public key of the user;

determining whether the current date/time is no more than a predetermined amount later than the freshness value;

independently computing the first hash;

verifying the first signature using the public key of the server and the independently computed first hash; and

if the results of the determining and verifying are positive:

forming a second signature of data from said package, derived from at least the first random number using the private key of the user; and sending the second signature via the network.

- value corresponding to a current date/time is formed; items are hashed including the first random number and the freshness value to form a first hash; a first signature of the first hash is formed using the private key of the server; a package including an encrypted component containing at least the first random number, freshness value, and first signature is sent to the user via the network; and subsequently there is received a second signature of data derived from at least the first random number, said second signature being formed using the private key of the user; and using the public key of the user, it is first verified whether the second signature is for the same first random number as was sent by the server. As an alternative embodiment of the invention, at least first, second, third, and fourth random numbers are generated and utilized in constructing the package. Specifically, in forming the package at the server, at least the first and second random numbers are contained in the encrypted component which is formed using the public key of the user and the third random number; the first hash is formed by hashing together the first and at least another of the random numbers contained in the package (including possibly the second random number) and the freshness value; the first signature of the first hash is formed using the private key of the server and the fourth random number. In regard to the subsequently received second signature of data, the data comprises a second hash which has been formed at the user equipment by hashing together the first and at least another of the random numbers contained in the package (including possibly the second random number), and the signature thereof has been formed using the private key of the user and the second random number. Then, the first verifying step is whether the second signature is for same random numbers as were sent by the server. This leaves the user equipment with at least the first random number which is fresh, secret, and consequently usable for a subsequent signature or encryption operation, while also enabling the server to authenticate the user by the fact that the user was able to sign the first and at least another random number included in the package using his private key and the second random number.

Brief Summary Text (22):
From the point of view of the user equipment, the present invention is directed to a method for obtaining and using secret fresh random numbers at user equipment in a networked environment to which a server is coupled, in which: an ID of a user is transmitted; a package is received including an encrypted component containing at least a first random number, which has been formed using the public key of the user, a freshness value corresponding to a date/time, and a first signature of a first hash, said first hash having been formed by hashing together items including said first random number and the freshness value, and said first signature having been formed using the private key of the server; at least the first random number is decrypted the using the private key of the user; it is determined whether the current date/time is no more than a predetermined amount later than the freshness value; the first hash is independently computed; the first signature is verified using the public key of the server and the independently computed first hash; and if the results of the determining and verifying are positive, a second signature of data derived from at least the first random number is formed using the private key of the user, and is sent to the server via the network.

Detailed Description Text (2):
It should be understood that while the present invention is discussed hereinafter in terms of an exemplary system and method for obtaining digitally signed documents of a plurality of users in a networked environment which have been signed employing the El-Gamal algorithm, the principles of the present invention are equally applicable to distribution of secret fresh random numbers, and/or to distribution of a combination of a secret fresh random number and an encrypted private key, for other purpose. Further, when used for digital signatures, it should be appreciated that such signatures may be applied to a variety of data, files, programs or other "documents", whether originated, modified or reviewed by users. In any event, the digital signature may be thought of as manifesting an approval by the user of a document.

Detailed Description Text (10):
User equipment 12 includes: input interaction means 12a such as a mouse and/or keyboard, handwriting recognition, voice recognition or other input means for obtaining an ID and, if used, a passphrase from a user, and for a user to fill in a document, and for biometric measurement or scanning, if used, to obtain biometric

information (fingerprint, voiceprint, retina scan, face scan) from a user; a hashing means for applying a secure hash function (SHA-1 or RIPEMD) to an entered passphrase or obtained biometric information, and to an approved document; a symmetric decryption means 12c for decrypting an encrypted private key received from server 16 using the hashed passphrase or biometric information as a user identifying key; and an El-Gamal algorithm means 12d for performing encryption, decryption, signature and verification operations in accordance with the El-Gamal algorithm, the encryption and signing operations requiring secret fresh random numbers. In particular, as will become clearer as the discussion proceeds, El-Gamal algorithm means performs decryption, verification, and signature operations in conjunction with a challenge response protocol assuring to the user equipment 12 that a random number R1 supplied to from server 16 is both secret and fresh, and assuring to the server that the user is in possession of the private key (i.e. was able to decrypt the private key because the correct user identifying information has been obtained by user equipment 12). Thereafter, a document is sent for approval, possibly after modification or filling in, a hash of the approved document is signed using the private key of the user and this secret fresh random number R1 to form a digital signature S[KprUser, R1](H(DOC)) of a document. The various hashing, symmetrical decryption, and El-Gamal algorithm means 12b, 12c, 12d may be implemented by software running on a CPU (not shown) of user equipment 12 or by special purpose hardware. Where the system 10 is implemented as an intranet, this functionality would be carried out by an applet supplied by server 16. It should be understood that in order to prevent a man-in-the-middle attack, the applet must be signed by the server and verified at user equipment 12 using the public key of the server KpuServer obtained with a certificate from a trusted authority.

Detailed Description Text (12):
The operation of the networked system 10 in providing a secret fresh random number R1 and encrypted private key KprUser to the user in the course of a phase in the nature of a challenge response protocol, which after completion of this phase, are used for a digital signature employing the El-Gamal algorithm of a document S[KprUser, R1](H(DOC)) which is derived from, or the same as, a then supplied document, will be best understood by also referring to FIG. 2. This Figure shows the operations performed by user interaction, by the user equipment 12, and by the server 16 in different columns. For the purposes of this Figure, it is assumed that the user has already requested access to the document system (home page) and the server 16 has sent a sign-in page to the user equipment 12. Thereafter at step 30, the user enters his ID in the sign-in page via input means 12a, e.g. the initials of the user, providing the IDs of all users are unique, and at step 40 the sign-in page including the entered ID is transmitted to the server, which receives it at step 70. In response, at step 72 the server 16, using the received ID as an index, reads from store 18 the corresponding encrypted private key E[Kpass](KprUser) and public key KpuUser of the user. Also at step 74, random number generator 16b generates four random numbers R1, R2, R3, and R4 and freshness value generating means 16e forms a freshness value FR representing the current date/time by checking the clock (not shown) of server 16.

Detailed Description Text (34):
In the combined random number passing and challenge response protocol of the present invention, the random numbers R1, R2 have been encrypted by the server to prevent an attacker from getting the numbers and discovering the user's private key KprUser from a signature or encryption by the user using the private key. The freshness value has been sent to assure the freshness of the encrypted random numbers. These random numbers R1, R2 and the freshness value FR have been signed by the server (in forming the first signature S1) to prove that:

CLAIMS:

1. A method of administration of secret fresh random numbers for use by users in a networked environment to which a server is coupled, there being associated with each user a unique respective set including an ID, a private key, and a public key corresponding to the private key, and with the server a private key and a public key, said method comprising, at the server:

receiving via the network a user's ID;

L7: Entry 1 of 2 File: EPAB Dec 10, 1998

PUB-NO: WO0009856179A1
DOCUMENT-IDENTIFIER: WO 9856179 A1
TITLE: CONDITIONAL ACCESS SYSTEM FOR SET-TOP BOXES

PUBN-DATE: December 10, 1998

INVENTOR-INFORMATION:

NAME	COUNTRY
ESKICIOGLU, AHMET MURSIT	US
WEHMEYER, KEITH REYNOLDS	US
VIRAG, DAVID EMERY	US

ASSIGNEE-INFORMATION:

NAME	COUNTRY
THOMSON CONSUMER ELECTRONICS	US
ESKICIOGLU AHMET MURSIT	US
WEHMEYER KEITH REYNOLDS	US
VIRAG DAVID EMERY	US

APPL-NO: US09811633
APPL-DATE: June 5, 1998

PRIORITY-DATA: US04881997P (June 6, 1997)

INT-CL (IPC): H04 N 7/167; H04 N 7/16; H04 N 5/00
EUR-CL (EPC): H04N007/16; H04N007/167

ABSTRACT:

CHG DATE=19990905 STATUS=O>A system conditionally establishes a communication channel between two devices only if one device is authenticated by the other device. Authentication of the second device by the first device involves sending a message to the second device; receiving, from the second device, the message encrypted using a private key of the second device and a digital certificate having a public key of the second device; decrypting the digital certificate to obtain the public key, using the public key to decrypt the message and comparing the decrypted message to the message originally sent to the second device.

WEST

End of Result Set

Generate Collection Print

L7: Entry 2 of 2 File: DWPI Oct 7, 1998

DERWENT-ACC-NO: 1998-508860
DERWENT-WEEK: 199844

TITLE: Digital certificate for authenticating association between user and public key of user - uses first set of data that comprises public key of user, and indicator identifying location for obtaining second set of data related to digital certificate

INVENTOR: ROMNEY, G; ZUBELDIA, P

PATENT-ASSIGNEE: ARCANVS (ARCAN)

PRIORITY-DATA: 1997US-0825876 (April 2, 1997)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
EP 869637 A2	October 7, 1998	E	010	H04L009/32

DESIGNATED-STATES: AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI

CITED-DOCUMENTS:No-SR.Pub

APPLICATION-DATA:

PUB-NO	APPL-DATE	APPL-NO	DESCRIPTOR
EP 869637A2	April 1, 1998	1998EP-0105970	

INT-CL (IPC): H04 L 9/32

ABSTRACTED-PUB-NO: EP 869637A
BASIC-ABSTRACT:

A digital certificate includes a first set of data related to the digital certificate. The first set of data comprises a public key of the user, and an indicator identifying a location for obtaining a second set of data related to the digital certificate. A digital signature comprises an encrypted message digest of the first set of data. The indicator comprises a unique user ID e.g. an Internet address with URL (Uniform Resource Locator) containing identifying information of a digital certificate.

The Internet address is the Internet address of a repository while the indicator is generated by a certificate issuer. The second set of data comprises a digital signature with encrypted message of the second set of data such as a period of validity.

USE - For authenticating association between user and public key of user.

ADVANTAGE - Allows change of certificate information without requiring re-issuance of new certificate.

ABSTRACTED-PUB-NO: EP 869637A
EQUIVALENT-ABSTRACTS:

CHOSEN-DRAWING: Dwg.1/10

DERWENT-CLASS: T01 W01
EPI-CODES: T01-D01; T01-H07C5E; W01-A05B;